

Course Outline

Implementing Cisco Security Monitoring, Analysis and Response System (MARS) v2.0

Duration: 2 days Virtual Classroom

2 days Classroom

Learning Objectives:

Cisco Security Mitigation and Response System (CS MARS) is a family of high performance, scalable appliances for threat management, monitoring and mitigation, enabling customers to make more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification and automated mitigation capabilities. CS MARS solutions empower customers to readily and accurately identify, manage and eliminate network attacks and maintain network compliance.

Target Audience:

- Employee
- Customer
- Channel Partners/Resellers

Prerequisites:

Fundamental knowledge of implementing network security / CCSP or Security CQS and working knowledge of routing and switching / CCNA

Topics Covered:

- MARS Introduction and Task Flow / Provide overview of MARS technology and STM Task Flow Overview.
- Lab 1-1 Accessing MARS 20 appliance.
- Configuring MARS, Configure administration tasks in the MARS system using User Interface.
- Lab 2-1 Adding Cisco Reporting Devices into MARS
- Lab 2-2 Adding non-Cisco Reporting Devices into MARS
- MARS Incident Investigation Configure MARS for incident investigation, create query and send alerts.
- Lab 3-1 Generating Summary Reports
- Lab 3-2 Configure appliance to perform Incident Investigation and attack mitigation.
- Lab 3-3 Creating Queries and Reports.
- MARS Rules and Management Use MARS User Interface to configure rules, management and system maintenance features.
- Lab 4-1 Distributed Threat Mitigation Lab
- Lab 4-2 Create a Custom Parser
- MARS Global Controller, Provide overview of MARS Global Controller